日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

#3

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ５月２９日

出 願 番 号
Application Number: 特願２０００－１５８７７０

出 願 人
Applicant (s): 株式会社日立製作所

U.S. Appln Filed 5-25-01
Inventor: T. Oishi et al
Mathingly Stanger & Malur
Docket ASH-1004

CERTIFIED COPY OF PRIORITY DOCUMENT

２００１年 ４月１３日

特 許 庁 長 官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２００１－３０２９５３０

【書類名】　特許願

【整理番号】　H00010271

【あて先】　特許庁長官殿

【国際特許分類】　G03F　3/00

H04L 12/00

【発明者】

【住所又は居所】　東京都小平市上水本町５丁目２２番１号　株式会社　日立超エル・エス・アイ・システムズ内

【氏名】　大石　敏久

【発明者】

【住所又は居所】　東京都青梅市新町六丁目１６番地の３　株式会社日立製作所　デバイス開発センタ内

【氏名】　戸澤　淳

【発明者】

【住所又は居所】　東京都青梅市新町六丁目１６番地の３　株式会社日立製作所　デバイス開発センタ内

【氏名】　柴山　哲也

【発明者】

【住所又は居所】　東京都小平市上水本町５丁目２２番１号　株式会社　日立超エル・エス・アイ・システムズ内

【氏名】　濱田　真人

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社　日立製作所

【代理人】

【識別番号】　100085811

【弁理士】

【氏名又は名称】　大日方　富雄

【電話番号】　03-3269-1430

【手数料の表示】

【予納台帳番号】　027177

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証通信用半導体装置

【特許請求の範囲】

【請求項１】　１個の半導体チップ上に、所定のアルゴリズムに従って鍵コードを生成するとともに外部装置とのデータの送受信の認可／非認可の決定並びに通信制御を行なう主処理部と、該処理部で生成された鍵コードを用いて送受信データの暗号化および復合化を行なう暗号処理部と、所定のプロトコルに従って上位層または下位層との通信を行なうインタフェース部とが形成されていることを特徴とする認証通信用半導体装置。

【請求項２】　１個の半導体チップ上に、所定のアルゴリズムに従って鍵コードを生成するとともに外部装置とのデータの送受信の認可／非認可の決定並びに通信制御を行なう主処理部と、該処理部で生成された鍵コードを用いて送受信データの暗号化および復合化を行なう暗号処理部と、所定のプロトコルに従って上位層との通信を行なう第１のインタフェース部と、所定のプロトコルに従って下位層との通信を行なう第２のインタフェース部とが形成されていることを特徴とする認証通信用半導体装置。

【請求項３】　上記主処理部は、鍵生成アルゴリズムおよびデータ送受信を要求する外部装置の認証を行なう認証アルゴリズムを具現化するプログラムを格納した不揮発性メモリと、上記プログラムに従って鍵コードを生成および外部装置とのデータの送受信の認可／非認可の決定を行なうプログラム実行型の制御手段と、該制御手段の作業領域を提供する揮発性メモリとから構成され、

上記不揮発性メモリ、上記制御手段、上記揮発性メモリ、上記暗号処理部および上記インタフェース部は内部バスを介して互いに接続されていることを特徴とする請求項１または２に記載の認証通信用半導体装置。

【請求項４】　上記暗号処理部は、上記主処理部で生成された鍵コードが設定されるレジスタを備え、該レジスタに上記バスを介して設定された鍵コードに基づいて送受信データの暗号化および復合化を行なうように構成されていることを特徴とする請求項３に記載の認証通信用半導体装置。

【請求項５】　上記インタフェース部は、通信制御コードが設定されるレジ

スタを備え、該レジスタに上記主処理部によって上記バスを介して設定された通信制御に基づいて通信を行なうように構成されていることを特徴とする請求項３または４に記載の認証通信用半導体装置。

【請求項６】　上記内部バスが結合された外部端子を備えていることを特徴とする請求項５に記載の認証通信用半導体装置。

【請求項７】　請求項６に記載の認証通信用半導体装置と、上記内部バスが結合された外部端子に接続された外部メモリとを備え、該外部メモリには通信路の設定を含む通信制御プログラムが格納され、該プログラムに従って上記主処理部が上記インタフェース部の上記レジスタに通信制御コードを設定することにより外部装置との通信が行なわれるように構成されていることを特徴とする電子機器。

【請求項８】　単一の半導体チップに形成され、暗号鍵コードによって暗号時は平文データを暗文データに暗合化し、復号時は暗文データを平文データに復号化し、暗号化および復号化の必要がない場合はデータをそのまま素通りさせる暗号処理部を備え、前記暗号処理部の暗文データには、通信の下位層とプロトコルを司る下位層インターフェース部が接続され、前記暗号処理部の平文データには、通信の上位層とプロトコルを司る上位層インターフェース部が接続され、前記下位層インターフェース部は、前記半導体チップの外部の通信信号を制御する下位層デバイスとの間で暗文データの伝送を行う下位層通信路を少なくともひとつ備え、前記上位層インターフェース部は、前記半導体チップの外部の上位層デバイスと平文データの伝送を行う上位層通信路を少なくともひとつ備え、下位層を経由する通信の認証処理および前記暗号処理部の鍵生成処理を行う鍵生成処理部を備え、前記鍵生成処理部はＣＰＵ、ＲＯＭ、ＲＡＭで構成され、前記ＣＰＵは、前記暗号処理部が暗号鍵を保持する鍵レジスタの設定と、前記下位層インターフェース部および上位層インターフェース部が備える制御レジスタの設定を、前記ＣＰＵ、前記暗号処理部、前記下位層インターフェース部および前記上位層インターフェース部とを接続するバスを経由して行なうように構成されていることを特徴とした認証通信用半導体装置。

【請求項９】　前記単一の半導体チップに形成され、前記半導体チップの前

記上位層インターフェース部に、更に暗号処理部を経由せず前記下位層インターフェース部から前記上位層インターフェース部に第１の上位層－下位層通信路と第２の上位層－下位層通信路が接続され、前記上位層インターフェース部は、前記半導体チップの外部の上位層デバイスとの間の信号伝送を行う第１の上位層通信路と第２の上位層通信路を備え、第１の上位層通信路は暗号処理部からのデータかあるいは暗号処理部を経由しない下位層インターフェースからのデータかを選択でき、第２の上位層通信路は前記第１の上位層－下位層通信路からのデータかあるいは前記第２の上位層－下位層通信路からのデータかを選択できることを特徴とする請求項８の認証通信用半導体装置。

【請求項１０】　前記単一の半導体チップに形成され、前記暗号処理部に第１の暗号処理回路と第２の暗号処理回路を備え、前記上位層インターフェース部に第１の上位層インターフェース回路と第２の上位層インターフェース回路を備え、前記第１の暗号処理回路の平文データの通信路を前記第１の上位層インターフェース回路に接続し、前記第２の暗号処理回路の平文データの通信路を前記第２の上位層インターフェース回路に接続し、前記第１の上位層インターフェースに前記半導体チップの外部の第１の上位層デバイスとの間の信号伝送を行う第１の上位層通信路と、前記第２の上位層インターフェースに前記半導体チップの外部の第２の上位層デバイスとの間の信号伝送を行う第２の上位層通信路とを備えることを特徴とする請求項８の認証通信用半導体装置。

【請求項１１】　前記バスに接続されて電気的に書換え可能な不揮発メモリが同一半導体チップ上に形成されていることを特徴とする請求項８の認証通信用半導体装置。

【請求項１２】　前記下位層デバイスを同一半導体チップ上に備え、前記下位層デバイスからの間の信号伝送を行う通信路を少なくともひとつ備えることを特徴とする請求項８の認証通信用半導体装置。

【請求項１３】　請求項８～１２のいずれかに記載の認証通信用半導体装置と、前記下位層デバイスと、該下位層デバイスと結合され外部から通信用伝送媒体が接続可能なコネクタとを備えたことを特徴とする電子機器。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データ処理技術さらには暗号鍵コードを用いたデシタルデータの暗号化／復号化処理に適用して有効な技術に関し、例えばＩＥＥＥ１３９４(Institute of Electrical and Electronics Engineers 1394)規格のシリアルバスを介して接続される電子機器の間で通信の安全性を保証しつつ送受信するための通信用半導体装置およびそれを用いたシステムに利用して有効な技術に関する。

【０００２】

【従来の技術】

ＩＥＥＥ１３９４規格は、音声や映像などのデシタルデータを、ケーブルを介してＡＶ機器などの電子機器間でシリアル伝送するための規格である。近年、ＩＲＤ(Integrated Receiver Decoder)やＤ－ＶＨＳ(Digital-VHS)、ＤＶ(Digital Video)カムコーダーなどの電子機器をＩＥＥＥ１３９４規格のシリアルバスを介して接続し、デジタル音声データやデジタル映像データなどのデジタルコンテンツを、例えばＩＳＯ／ＩＥＣ(International Standardization Organization/International Electrotechnical Commission)13818規格のMPEG2-TS(Moving Picture Experts Group 2 Tranport Stream)やIEC61883規格に準拠したパケットなどに乗せて送受信を行うことができるようにした電子機器が提案されている。

【０００３】

ところで、映画などの著作物を記憶するデシタルビデオテープやディスク等のメディアおよびその再生装置においては、著作権の保護の見地から違法なコピーを防止するための技術が不可欠である。近年、デジタルコンテンツの著作権保護のため、不正コピー防止技術が、例えば家電業界、パソコン業界および映画業界などが組織する業界団体であるＣＰＴＷＧ(Copy Protection Technical Working Group)などで標準化が進められている。ＣＰＴＷＧが中心となって決めた不正コピー防止技術では、DVD-VideoのＣＳＳ(Content Scrambling System)仕様やＩＥＥＥ１３９４向けの５Ｃ-ＤＴＣＰ(5 Company Digital Transmission Copy Protection)仕様が、現在実用化されている。

【０００４】

しかしながら、DVD-Videoの不正コピー防止技術であるＣＳＳに関しては、クラッカー（悪意をもって不正アクセスなどを行うハッカーのこと）などによりＣＳＳのセキュリティを破るソフトウェアが作られ、米国やフランスなどで、インターネット上の複数のＷＷＷサーバで配布され産業界に深刻な打撃を与えている（日経ＢＰ社発行、日経エレクトロニクス、1999.11.1、No756、第23頁参照）。そのため、ＣＳＳや5C-ＤＴＣＰのようにセキュリティ技術が標準化され全く同じ技術を使用したＡＶ機器が大量に出回る場合は、クラッカーの不正コピー防止攻撃に対する安全性の高さが、デジタルコンテンツの著作権保護の観点からＡＶ機器に対し求められている(日経ＢＰ社発行、日経エレクトロニクス、2000.3.27、No766、P152～P163参照)。

【０００５】

また、著作物不正コピーの悪質な例では、ＣＤ(Compact Disc)に収められたゲームソフトの不正コピーを可能とするためのハード的な改造を某社製のゲーム機器に施したものが不正に売買されており、ゲームソフトの著作権保護が破られている。このように、近年においては、ソフトウェアによる不正コピーのみならず、電子機器のハードウェアの改造による手段に及んでまで不正コピー防止技術に対する攻撃の可能性がある（技術評論社発行、「暗号のすべてがわかる本」、初版第１刷、第126～128頁参照）。

【０００６】

一方、５Ｃ－ＤＴＰＣに関しては、以下のようなシステムが実用化されている。図１３に、従来の５Ｃ－ＤＴＰＣ仕様の認証通信装置とそれを用いたシステムとしてのＡＶ機器の概略構成を示す。図１３において、符号７２で示されているのは５Ｃ－ＤＴＰＣ仕様の通信用半導体装置（通信装置）、７１は認証処理を行なうマイクロコンピュータチップからなる認証装置である。該認証装置７１と上記通信装置７２は、デシタルビデオテープレコーダやセットトップボックスなどのＡＶ機器に搭載される。

【０００７】

通信装置７２は、図１３に示されているように、ＩＥＥＥ１３９４シリアルバス７３１との接続を行なう下位層インタフェース回路１００と、外部デバイスと

の接続を行なう上位層インタフェース回路２００と、暗号処理回路３００とからなり、ＩＥＥＥ１３９４規格のケーブル７３０が接続されるポート７１１～７１３を有する物理層としての１３９４ＰＨＹチップ７００とＭＰＥＧ２デコーダやコーデック、ＤＶコーデックなどを有するディスプレイ装置のような外部デバイス９０との間に接続されて、ＩＥＥＥ１３９４ケーブル７３０から送られてくる暗号化されたデジタルデータを復号化して外部デバイス９０へ伝える機能を有する。下位層インタフェース回路１００と上位層インタフェース回路２００と暗号処理回路３００は別のチップで構成されることもある。認証装置７１は、通信装置７２と外部バス４１を介して接続され、暗号処理回路３００で必要とされる暗号鍵コード（以下、単に暗号鍵と称する）を生成したりデータを受信したいＡＶ機器からの要求に応じて認証処理を行なう機能を有する。

【０００８】

【発明が解決しようとする課題】

しかしながら、上記従来の５Ｃ－ＤＴＰＣ仕様のシステム（認証通信装置）にあっては、通信装置７２が認証装置７１とは別のチップで構成されており、バス４１を介して認証装置７１やＲＡＭ７５０、電気的に書換え可能なフラッシュＲＯＭ７４０と接続されていた。そして、通信装置７２内のインタフェース回路１００と２００にはそれぞれ制御用レジスタ１４，２４が、また暗号処理回路３００には鍵レジスタが３４設けられており、これらのレジスタにバス４１を介して制御データや暗号化／復号化用の暗号鍵コードが認証装置７１によって設定されることで、暗号化、復号化処理などの動作を行なうように構成されていた。

【０００９】

そのため、上記従来の５Ｃ－ＤＴＰＣ仕様の認証通信装置は、暗号処理回路３００とバス４１とが接続される外部端子６２の信号を監視することで、秘匿性を有する暗号鍵が知られてしまったり暗号処理のアルゴリズムが解析されてしまうおそれがある。具体的には、図１０のＡＶ機器の構成において、ロジック・アナライザなどの計測機器を用いて、通信装置７２の外部端子６２の信号やＣＰＵバス４１のバス上のデータがモニタされるなどして、認証動作過程での通信コマンド、暗号交換鍵および乱数値などが窃取されることにより認証装置のセキュリテ

ィへの攻撃の手掛かりを得るための解析ができる余地を許している。

【００１０】

前記攻撃により認証動作を不正に回避する不正装置が作成された場合、例えば、図１４のようにＡＶ機器８００Ａおよび８００Ｂに、それぞれＣＰＵバス４１と認証装置７１に接続された不正装置７５を設けるとともに、各ＣＰＵバス４１－４１間にジャンパー線４６等の不正な接続線を設けるなどの改造がなされ、認証動作過程の通信コマンドが不正装置７５からそれぞれの認証装置７１へ発行されることで正規の認証が回避され、認証を不正に成立させる。その後、デジタルコンテンツが暗号処理回路３００で暗号化および復号化される段階では、各不正装置７５が認証装置７１へ、ＣＰＵバス４１のバス権を譲るように要求するバス権要求信号の発行を行なって、認証装置７１からＣＰＵバス４１のバス権を奪った後、正常の認証成立後に使用される暗号鍵の代わりとして、不正装置７５間で共有する不正鍵を使用することで、デジタルコンテンツがＡＶ機器８００Ａから８００Ｂへ不正に送信されるおそれがあるという課題があることが明らかとなった。

【００１１】

本発明の１つの目的は、外部端子を監視していても暗号鍵や制御データを読み取ることができないようにして、悪質なアクセスを行うクラッカーによるデジタルコンテンツの著作権保護のための不正コピー防止技術に対する攻撃手掛かりとなる解析を抑止してデジタルコンテンツの不正なコピーを防止可能な認証通信装置を提供することにある。

【００１２】

また、本発明の他の目的は、ハードウェアの改造により不正コピー防止技術が破られることを抑止するための認証通信装置を提供することにある。

【００１３】

この発明の前記ならびにそのほかの目的と新規な特徴については、本明細書の記述および添附図面から明らかになるであろう。

【００１４】

【課題を解決するための手段】

本願において開示される発明のうち代表的なものの概要を説明すれば、下記のとおりである。

【００１５】

すなわち、上記課題を解決するために、本発明の認証通信用半導体装置は、１個の半導体チップ上に、所定のアルゴリズムに従って鍵コードを生成するとともに外部装置とのデータの送受信の認可／非認可の決定並びに通信制御を行なう主処理部と、該処理部で生成された鍵コードを用いて送受信データの暗号化および復合化を行なう暗号処理部と、所定のプロトコルに従って上位層または下位層との通信を行なうインタフェース部とを形成したものである。

【００１６】

より具体的には、単一の半導体チップに形成され、暗号鍵コードによって暗号時は平文データを暗文データに暗合化し、復号時は暗文データを平文データに復号化し、暗号化および復号化の必要がない場合はデータをそのまま素通りさせる暗号処理部を備え、前記暗号処理部の暗文データには、通信の下位層とプロトコルを司る下位層インターフェース部が接続され、前記暗号処理部の平文データには、通信の上位層とプロトコルを司る上位層インターフェース部が接続され、前記下位層インターフェース部は、前記半導体チップの外部の通信信号を制御する下位層デバイスとの間で暗文データの伝送を行う下位層通信路を少なくともひとつ備え、前記上位層インターフェース部は、前記半導体チップの外部の上位層デバイスと平文データの伝送を行う上位層通信路を少なくともひとつ備え、下位層を経由する通信の認証処理および前記暗号処理部の鍵生成処理を行う鍵生成処理部を備え、前記鍵生成処理部はＣＰＵ、ＲＯＭ、ＲＡＭで構成され、前記ＣＰＵは、前記暗号処理部が暗号鍵を保持する鍵レジスタの設定と、前記下位層インターフェース部および上位層インターフェース部が備える制御レジスタの設定を、前記ＣＰＵ、前記暗号処理部、前記下位層インターフェース部および前記上位層インターフェース部とを接続するバスを経由して行なうように構成したものである。

【００１７】

上記した手段によれば、半導体チップの内部信号を外部から窃取しにくいとと

もに、認証処理過程の通信コマンドや暗号処理過程の暗号鍵設定を認証通信用ＬＳＩの外部から改竄して入力することが困難であるので、不正コピー防止技術を破るために認証処理過程を解析することが困難となり、また、電子機器を改造して不正コピー防止技術を破ることが難しくなり、これによって、著作権保護を必要とするデジタルコンテンツを高い安全性の下に送受信できる電子機器を実現することができる。

【００１８】

また、当該半導体装置が搭載される電子機器の固有情報等を記憶するための電気的に書き換え可能な不揮発性メモリを必要とする場合に、その不揮発性メモリも同一チップ上に形成する。これにより、当該電子機器の固有情報を、外部から窃取されるのを防止することができる。また、電気的に書き換え可能な不揮発性メモリであるため、機器毎に異なる固有情報を書き込むことでセキュリティを向上させることが容易であり、かつ低コストで済む。この不揮発性メモリは、予め固有情報を書込んだ状態で機器に組み込むようにすることができる。

【００１９】

さらに、鍵コードの生成や外部装置の認証並びに通信制御を行なう上記主処理部と上記暗号処理部および上記インタフェース部とが内部バスを介して互いに接続されており、当該半導体装置が搭載される電子機器の固有情報等を記憶するための電気的に書き換え可能な不揮発性メモリを必要とする場合に、その不揮発性メモリが接続される外部端子と上記内部バスとの間にバスの切換えを制御するバス制御回路を設ける。これにより、暗号処理過程や認証処理過程が外部から窃取されるのを防止することができるとともに、暗号処理過程での暗号鍵や認証処理過程の通信制御コードをチップの外部から改竄して入力することが困難となり、クラッカーによる暗号処理や認証処理の解析および装置の改造といった攻撃を抑止することが可能となり、著作権保護を必要とするデジタルコンテンツの不正コピーに対する安全性が高まる。

【００２０】

さらに、当該半導体装置が搭載される電子機器のシステム全体を制御するホストＣＰＵが別途必要であり、当該半導体装置の上記主処理部が、鍵生成アルゴリ

ズムおよびデータ送受信を要求する外部装置の認証を行なう認証アルゴリズムを具現化するプログラムを格納した不揮発性メモリと、上記プログラムに従って鍵コードを生成および外部装置とのデータの送受信の認可／非認可の決定を行なうプログラム実行型の制御手段と、該制御手段の作業領域を提供する揮発性メモリとから構成されているような場合に、上記制御手段とホストＣＰＵとの間の通信を行なう通信回路をホストＣＰＵとの通信ポートと上記内部バスとの間に設ける。これによって、ホストＣＰＵとの通信ポートを有する半導体装置において、当該通信ポートから暗号処理過程や認証処理過程が外部から窃取されるのを防止することができるとともに、暗号処理過程での暗号鍵や認証処理過程の通信制御コードをチップの外部から改竄して入力することが困難となり、クラッカーによる暗号処理や認証処理の解析および装置の改造といった攻撃を抑止することが可能となる。

【００２１】

しかもこの場合、上記制御手段は、限られた所定のコマンド以外を受付けないように構成する。これにより、暗号処理過程や認証処理過程でチップ外部から不正な介入を行なうことが困難となり、安全性が向上する。

【００２２】

【発明の実施の形態】

以下、本発明の好適な実施例を図面に基づいて説明する。

【００２３】

図１は、本発明を適用した５Ｃ－ＤＴＰＣ仕様の認証通信用ＬＳＩ（大規模半導体集積回路）の第１の実施形態を示す。

【００２４】

本実施例においては、中央処理ユニットＣＰＵ５００および作業領域を提供するＲＡＭ５０２、プログラムや固定データを格納するＲＯＭ５０１からなり暗号鍵を生成したり外部の装置との間のデータの送受信の認可／非認可を決定するための認証処理や通信制御などの機能を有する鍵生成＆認証処理部５０と、ＩＥＥＥ１３９４シリアルバスとの接続を行なう下位層インタフェース部１０と、外部デバイスとの接続を行なう上位層インタフェース部２０と、暗号鍵を用いてデー

タの暗号化および復合化処理を行なう暗号処理部３０と、これらの回路間を接続する内部バス４１とが、単結晶シリコンのような１個の半導体チップ上に形成され、認証通信用ＬＳＩを構成している。

【００２５】

さらに、通信路の設定などの通信制御プログラムや機器に関する固有情報等を記憶するための電気的に書換え可能なフラッシュメモリのような不揮発性の外部メモリ７４０が上記内部バス４１と接続されているとともに、上記下位層インタフェース部１０にはＩＥＥＥ１３９４規格のケーブル７３０が接続されるポート７１１～７１３を有する物理層としての１３９４ＰＨＹ(IEEE1394 Physical Layer Protocol)チップ７００が、また上位層インタフェース部２０にはＭＰＥＧ２デコーダやコーデック、ＤＶコーデックなどの外部デバイス９０を記録再生装置４０が接続されて、ＡＶ機器が構成される。

【００２６】

下位層インターフェース部１０は、パケット形態でデータの送受信を行なえるようにデータを処理するパケット処理回路１０１と、下位層バス１２を介して１３９４ＰＨＹチップ７００と接続されＩＥＥＥ１３９４ケーブルとの接続のための制御を行なうリンク層としての１３９４リンク回路１００と、で構成される。１３９４ＰＨＹチップ７００は、データのマルチプレックスやデマルチプレックスなど物理層としての制御を行なう半導体チップで、特に制限されるものでないが、本実施例では３つのＩＥＥＥ１３９４仕様のポート７１１，７１２および７１３を備えている。これらのポートとＩＥＥＥ１３９４仕様のケーブル（以下、１３９４ケーブルと称する）との具体的な接続の仕方は、図１３の従来例と同様である。すなわち、各ポート７１１，７１２および７１３は、それぞれＩＥＥＥ１３９４仕様のソケット７２１，７２２および７２３からなるコネクタ部７２０に接続されている。

【００２７】

ユーザは、ＩＥＥＥ１３９４コネクタ部７２０の空きソケットの何れか、例えばソケット７２１に１３９４ケーブル７４１の一端である１３９４プラグ７３１を接続し、非接続側の一端である１３９４プラグ７５１を他のＡＶ機器のＩＥＥ

Ｅ１３９４コネクタ部に接続することで、図７に示すようにＡＶ機器８００Ａと８００Ｂとの間でデジタルコンテンツおよび通信コマンドを送受信するための伝送路としての１３９４バス８１０を確保できる。また、１３９４ケーブル７４１のプラグ７３１をこのソケット７２１から引き抜くことで、当該ＡＶ機器を１３９４バスから解放することができる。なお、図７のＡＶ機器間の１３９４バスの接続図では、説明を簡単にするため２つのＡＶ機器で説明を進めるが、本発明は下位層の通信プロトコルで規定されるバスのトポロジーが２つに限定されるものでなく、１３９４バス８１０上には、他の電子機器が同様にして接続される。

【００２８】

上位層インターフェース回路２００は、１３９４ＰＨＹチップ７００の物理層や１３９４リンク回路１００のリンク層より上位の層へデジタルコンテンツを渡すためのインターフェース回路で、上位層バス２２を介してＭＰＥＧ２ ＣＯＤＥＣ（CODER DECODER）やＤＶ ＣＯＤＥＣなどの外部デバイス９０と接続され、外部デバイス９０は記録再生装置４００へ接続される。記録再生装置４００では、映像や音声のデジタルコンテンツを記録または再生する。

【００２９】

上記インタフェース部１０と２０にはそれぞれ制御用レジスタ１４，２４が設けられており、鍵生成＆認証処理部５０のＣＰＵ５００が内部バス４１を介して制御レジスタ２４および１４に制御コードを設定することで、１３９４リンク回路１００および上位層インターフェース回路２００の通信路の設定を行う。下位層の通信制御プログラムは外部メモリ７４０に格納されており、ＣＰＵ５００は、外部メモリ７４０内の下位層の通信制御プログラムに従って制御レジスタ１４を設定し、下位層デバイスを経由して１３９４バス８１０上の電子機器との通信を行う。具体的には、１３９４バス上の電子機器へ通信コマンドを発行し、例えばその電子機器の録画、再生、電源のオン/オフなどを制御したりその電子機器の情報を閲覧したりする。

【００３０】

上記暗号鍵処理部３０には鍵レジスタ３４が設けられており、また、ＲＯＭ５０１には暗号鍵生成アルゴリズムおよび認証アルゴリズムをそれぞれ具現化する

プログラムが格納されていて、鍵生成＆認証処理部５０のＣＰＵ５００は、ＲＯＭ５０１内の暗号鍵生成アルゴリズムに従って暗号鍵を生成し、生成した暗号鍵を暗号処理回路３００の鍵レジスタ３４へ書き込む。また、ＣＰＵ５００は、認証アルゴリズムに従って認証処理を行なう。

【００３１】

以下、図８を用いて上記実施例の認証通信用ＬＳＩを備えたＡＶ機器間の認証処理および暗号処理の手順を詳細に説明する。

【００３２】

記録再生装置４００に蓄積または伝送されるデジタルコンテンツをＡＶ機器８００ＡからＡＶ機器８００Ｂへ送信する際には、先ず暗号化されたデジタルコンテンツを受信したいＡＶ機器８００Ｂから１３９４バスを介してＡＶ機器８００Ａに対して認証を要求する通信コマンドに機器の情報を付加して送信する。認証要求コマンドを受信したＡＶ機器８００ＡのＣＰＵ５００は、ＲＯＭ５０１に記録されている認証処理プログラムを実行して認証処理を行い、認証処理が成功した場合はその電子機器を不正ではない電子機器であると認知する。

【００３３】

認証が成立すると、ＡＶ機器８００Ａの鍵生成＆認証処理部５０おいて、デジタルコンテンツの暗号鍵Ｋcontを、ＡＶ機器８００Ｂで生成するために必要な情報である乱数値seedおよび認証鍵Ｋauthを用いて交換鍵Ｋｘに変換する暗号化処理を行なって暗号交換鍵Ｋｓｘを生成して、ＣＰＵバス４１－１３９４リンク回路１００１３９４－ＰＨＹチップ７００－１３９４バス８１０を介してＡＶ機器８００Ｂへ送信する。

【００３４】

一方、ＡＶ機器８００Ｂでは１３９４バス８１０からの通信コマンドを、１３９４ＰＨＹチップ７００、１３９４リンク回路１００およびＣＰＵバス４１を経由して鍵生成＆認証装置５０に渡し、受信した乱数値seedおよび暗号交換鍵Ｋｓｘを、自己が保有している認証鍵Ｋauthを用いて復号する復号処理を行ない、復号された交換鍵Ｋｘを用いてＡＶ機器８００Ａ側の暗号鍵Ｋcontと同一の暗号鍵Ｋcontを得ることで、自電子機器と相手電子機器で交換鍵Ｋｘを共有する。

【００３５】

続いて、ＡＶ機器８００Ａは、ＲＯＭ５０１に記録されている鍵生成処理プログラムを実行して、交換鍵Ｋｘおよび乱数値seedから暗号鍵Ｋcontを生成し、暗号処理回路３００の鍵レジスタ３４へ設定する。すると、暗号処理回路３００は、自機器の外部デバイス９０から入力される例えばＭＰＥＧ２-ＴＳパケットに乗せられた平文データからなるデジタルコンテンツを、上記暗号鍵Ｋcontを用いて暗号化し、暗号文データとして出力し、パケット処理回路１０１に設けられているバッファ（図示省略）に蓄え、ＩＥＥＥ１３９４で規定されるパケットの構築を行う。このとき、前記バッファは１３９４バス８１０への転送が１３９４リンク回路１００で可能となるまで保持することで、上位層バス２２の伝送速度と下位層バス１２の伝送速度の相違を吸収する緩衝メモリの役割を果たす。

【００３６】

そして、１３９４リンク回路１００が１３９４バス８１０へのデータ転送が可能な状態となった時点で下位層バス１２から１３９４ＰＨＹチップ７００へ前記デジタルコンテンツが暗号化された１３９４パケットデータを出力し、１３９４ＰＨＹチップ７００は１３９４バス８１０を経由して、相手ＡＶ機器へデジタルコンテンツの伝送を開始する。さらに、ＡＶ機器８００Ａは、相手ＡＶ機器８００Ｂで復号するための情報として乱数値seedを、１３９４バス８１０を経由してＡＶ機器８００Ｂへ送信する。ＡＶ機器８００Ｂでは、認証鍵Ｋauthを用いて暗号交換鍵Ｋｓｘを復号した交換鍵Ｋｘおよび受信した前記乱数値seedを用いて、自機器の鍵生成＆認証処理部５０で自機器のＲＯＭ５０１内の鍵生成処理アルゴリズムに従って、受信した暗号化デジタルコンテンツを暗号処理回路３００で復号化させる処理を行う。そして、復号されたデジタルコンテンツは、外部デバイス９０を介してＡＶ機器８００Ｂの記録再生装置４００へ記録または再生される。

【００３７】

上記第１実施形態の認証通信用ＬＳＩにおいては、一連の処理の間、認証処理過程および鍵生成処理過程で発生するＲＯＭ５０１のプログラムアクセスに伴なうデータおよびＣＰＵ作業中にＲＡＭ５０２へ格納される一時データが、ＣＰＵ

バス４１上に乗ることになるが、従来は別チップで構成されていた認証処理装置と暗号処理装置とが一つの半導体チップ上に形成されているため、暗号処理装置の外部端子を直接観測する場合に比べて外部からのバスの観測のみでチップ内の処理過程の細部を解析することが困難になる。

【００３８】

また、実施例の認証通信用ＬＳＩは、鍵レジスタ３４への設定が、唯一ＣＰＵ５００から行えるようにＣＰＵバス４１が制御されるように構成することができる。そのため、外部からＣＰＵバス４１への入力で鍵レジスタ３４を設定することができないので、認証通信用ＬＳＩを搭載した機器の改造が困難になる。さらに、１チップ化されたことにより、コストダウンが図れるとともに、機器の部品点数を減らし、実装密度を高めることができる。

【００３９】

図２は、本発明の第２の実施形態を示す。この第２の実施形態は第１の実施形態とほぼ同様な構成を備えており、異なる点は、①下位層インターフェース部１０に異種のパケット処理例えばＭＰＥＧ２－ＴＳのパケット構築を行う第１のパケット処理回路１０１と、ＩＥＣ６１８８３のような暗号化が不要なデジタルコンテンツのパケット構築を行う第２のパケット処理回路１０２と、ＡＮＳＩ(American National Standard Institute) ＮＣＩＴＳ 325-1998 で規格が進められているＳＢＰ－２(Serial Bus Protocol 2)のようなデジタルデータのパケット構築を行う第３のパケット処理回路１０３とを備え、暗号化が不要なデジタルコンテンツは伝送線２１１，２１２を介して直接パケット処理回路１０２または１０３と上位層インターフェース部２０との間で伝送されるように構成されている点と、②上位層インターフェース部２０が、暗号処理回路３００からのパケットまたは第２のパケット処理回路１０２からのパケットを選択して上位層バス２２１への伝送を可能とする上位層インターフェース回路２０１と、第２のパケット処理回路１０２からのパケットまたは第３のパケット処理回路１０３からのパケットを選択して上位層バス２２２への伝送を可能とする上位層インターフェース回路２０２とで構成されている点と、③上位層インターフェース回路２０１，２０２を介して複数の外部デバイス９０～９３を同時に接続できるように構成され

ている点の３つである。この実施例では、パケット処理回路１０２，１０３と１３９４リンク回路１００とはバス１１１によって接続されている。また、パケット処理回路１０２と上位層インターフェース回路２０１，２０２はバス２１１によって接続されている。パケット処理回路１０３と上位インターフェース回路２０２はバス２１２によって接続されている。他の構成および各種処理の手順並びに作用効果は第１の実施形態と同様であるので、説明は省略する。

【００４０】

図３は、本発明の第３の実施形態を示す。この第３の実施形態は第１の実施形態とほぼ同様な構成を備えており、異なる点は、①暗号処理部３０に２つの暗号処理回路３００および３０２を備えるとともに、下位層インターフェース部１０に例えばＭＰＥＧ２－ＴＳのパケット構築を行う２つのパケット処理回路１０１、１０４を、また上位層インターフェース部２０は暗号処理回路３００，３０２に対応して第１および第２の上位層インターフェース回路２００，２０３を備え、暗号化を必要とするデジタルコンテンツの転送を２系統同時に行なえるように構成されている点と、②上位層インターフェース回路２００，２０３を介して複数の外部デバイス９１，９２を同時に接続できるように構成されている点の２つである。他の構成および各種処理の手順並びに作用効果は第１の実施形態と同様であるので、説明は省略する。

【００４１】

図４は、本発明の第４の実施形態を示す。この第４の実施形態は、第１の実施形態においてチップの外部に設けられていた電気的に書換え可能な不揮発性メモリ７４０を内部不揮発性メモリ５０３として設けたものである。

【００４２】

第１～第３の実施形態の認証通信用ＬＳＩにおいては、チップの外部に設けられたメモリ７４０が内部バス４１に接続されており、認証処理から鍵生成処理までの一連の処理の間、認証処理過程および鍵生成処理過程で発生するＲＯＭ５０１のプログラムアクセスに伴なうデータおよびＣＰＵ作業中にＲＡＭ５０２へ格納される一時データがＣＰＵバス４１上に乗るため外部から観測できることとなるが、図４の実施形態の認証通信用ＬＳＩ７０では、ＣＰＵバス４１がチップの

外部端子と接続されないように構成されているため、処理過程をチップ外部から観測されることはない。また、鍵レジスタ３４への設定は、唯一ＣＰＵ５００から行えるようにＣＰＵバス４１が制御されるように構成されているため、外部からＣＰＵバス４１への入力で鍵レジスタ３４を設定することはできないため、改造が困難である。

【００４３】

図５は、本発明の第５の実施形態を示す。この第５の実施形態は、第１の実施形態においてチップの外部に設けられていた下位層デバイスである１３９４ＰＨＹ回路７００を認証通信用ＬＳＩ７０と同一チップ内に設けたものである。１３９４ＰＨＹ回路７００も含めて１チップ化されたことにより、さらにコストダウンが図れるとともに、機器の部品点数を減らし、より一層実装密度を高めることができる。

【００４４】

図６は、本発明の第６の実施形態を示す。第６の実施形態は、内部不揮発性メモリ５０３をチップ内部に設けた第４の実施形態の認証通信用ＬＳＩ７０において、さらに１３９４ＰＨＹ回路７００をも同一チップ内に設けたものである。この実施形態によれば、第４の実施形態の有する効果に加えて第５の実施形態の有する効果をも奏することができる。

【００４５】

図９は、本発明を適用した５Ｃ－ＤＴＰＣ仕様の認証通信用ＬＳＩの他の実施形態を示す。この実施形態では、図１の実施形態のＬＳＩにさらにシステム全体を制御するホストＣＰＵ８２との間のシリアル通信を行なう通信回路８０と、外部メモリ７４０と内部バス４１との接続切換えなどの制御を行なうバス制御回路６０とを設けたものである。図に示されているように、通信回路８０は内部バス４１とホストＣＰＵ８２との間に設けられており、シリアル通信線８１を介してホストＣＰＵ８２と接続されている。また、外部メモリ７４０は外部バス６１を介してバス制御回路６０に接続されている。

【００４６】

このように、本実施例においては、内部バス４１がバス制御回路６０と通信回

路８０とにより外部から分離されており、内部バス上の信号を直接外部端子からモニタすることができない構成とされている。これによってデータの秘匿性が向上されるとともに、クラッカーによる認証アルゴリズムや暗号鍵生成アルゴリズムの解析を一層困難にすることができる。さらに、本実施例においては、内部ＣＰＵ５００はホストＣＰＵ８２からの所定のコマンド以外を受けつけないように構成されており、ＣＰＵ５００に不正なコマンドを与えてＲＡＭ５０２やＲＯＭ５０１のデータをチップ外部に読み出すようなことができない構成とされている。

【００４７】

図１０は、本発明を適用した認証通信用ＬＳＩのさらに他の実施形態を示す。この実施形態では、図９の実施形態のＬＳＩにおけるホストＣＰＵ８２との間のシリアル通信を行なう通信回路８０を省略し、外部メモリ７４０と内部バス４１との間にバスの接続切換えなどの制御を行なうバス制御回路６０を設けたものである。

【００４８】

図１１は、本発明を適用した認証通信用ＬＳＩのさらに他の実施形態を示す。この実施形態では、図９の実施形態のＬＳＩにおけるホストＣＰＵ８２との間のシリアル通信を行なう通信回路８０を省略し、外部メモリ７４０と内部バス４１との間にバスの接続切換えなどの制御を行なうバス制御回路６０を設けるとともに、上位層と下位層の外部インタフェース回路１０，２０のうち下位層の外部インタフェース回路１０のみを設けたものである。

【００４９】

図１２は、本発明を適用した認証通信用ＬＳＩのさらに他の実施形態を示す。この実施形態では、図９の実施形態のＬＳＩにおけるホストＣＰＵ８２との間のシリアル通信を行なう通信回路８０を省略し、外部メモリ７４０と内部バス４１との間にバスの接続切換えなどの制御を行なうバス制御回路６０を設けるとともに、上位層と下位層の外部インタフェース回路１０，２０のうち上位層の外部インタフェース回路２０のみを設けたものである。

【００５０】

図１０～図１２の実施形態においても、内部バス４１がバス制御回路６０によって外部バス６１と切り離されているので、不正コピー防止上、図９の実施形態の認証通信用ＬＳＩとほぼ同様の利点を有している。また、図１１および図１２の実施形態のように、暗号生成＆認証処理部５０と暗号処理部３０と上位層と下位層の外部インタフェース回路１０，２０のうち一方とが１つのチップ上に形成されていれば、暗号処理部３０に入出力される平文データと暗文データを直接対比して暗号鍵を推定することができないため、データの秘匿性を高めることができる。

【００５１】

以上本発明者によってなされた発明を実施例に基づき具体的に説明したが、本発明は上記実施例に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。例えば図４～図１２の実施例において、図２や図３の実施例のように、複数のパケット処理回路や複数の上位インタフェース回路を設けて、複数のパケットデータの転送を同時に行なえるように構成しても良い。　以上の説明では主として本発明者によってなされた発明をその背景となった利用分野である５Ｃ－ＤＴＰＣ仕様の認証通信用ＬＳＩに適用下場合について説明したが、本発明はDVD-VideoのＣＳＳ仕様の通信用ＬＳＩにも利用することができる。また、本発明を適用した認証通信用ＬＳＩは、デシタルビデオテープレコーダやＩＲＤ（Integrated Receiver／Decoder）などのＡＶ機器のみならずパーソナルコンピュータなどにも利用することができる。

【００５２】

【発明の効果】

本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば下記のとおりである。　すなわち、本発明に従うと、半導体チップの内部信号を外部から窃取しにくいとともに、認証処理過程の通信コマンドや暗号処理過程の暗号鍵設定を認証通信用ＬＳＩの外部から改竄して入力することが困難であるので、不正コピー防止技術を破るために認証処理過程を解析することが困難となり、また、電子機器を改造して不正コピー防止技術を破ることが難しくなり、これによって、著作権保護を必要とするデジタルコンテンツを高い安全

性の下に送受信できる電子機器を実現することができる。

【図面の簡単な説明】

【図１】

本発明を適用した認証通信用ＬＳＩおよびそれを搭載したＡＶ機器の第１の実施形態を示すブロック図である。

【図２】

本発明を適用した認証通信用ＬＳＩおよびそれを搭載したＡＶ機器の第２の実施形態を示すブロック図である。

【図３】

本発明を適用した認証通信用ＬＳＩおよびそれを搭載したＡＶ機器の第３の実施形態を示すブロック図である。

【図４】

本発明を適用した認証通信用ＬＳＩおよびそれを搭載したＡＶ機器の第４の実施形態を示すブロック図である。

【図５】

本発明を適用した認証通信用ＬＳＩおよびそれを搭載したＡＶ機器の第５の実施形態を示すブロック図である。

【図６】

本発明を適用した認証通信用ＬＳＩおよびそれを搭載したＡＶ機器の第６の実施形態を示すブロック図である。

【図７】

図１の構成を有する２つのＡＶ機器をＩＥＥＥ１３９４シリアルバスに接続した場合の説明図である。

【図８】

本発明を適用した認証通信用ＬＳＩおよびそれを搭載したＡＶ機器における認証処理および暗号処理の過程説明図である。

【図９】

本発明を適用した認証通信用ＬＳＩおよびそれを搭載したＡＶ機器の第７の実施形態を示すブロック図である。

【図１０】

図９の実施形態の変形例を示すブロック図である。

【図１１】

図９の実施形態の変形例を示すブロック図である。

【図１２】

図９の実施形態の変形例を示すブロック図である。

【図１３】

従来の認証通信装置およびそれを搭載したＡＶ機器の一例を示すブロック図である。

【図１４】

従来の認証通信装置を用いたＡＶ機器における不正改造の例を示す説明図である。

【符号の説明】

１０　下位層インターフェース部

１４　制御レジスタ

２０　上位層インターフェース部

２４　制御レジスタ

３０　暗号処理部

３４　鍵レジスタ

４１　内部バス

５０　鍵生成＆認証処理部

７０　認証通信装置

９０～９３　外部デバイス

１００　１３９４規格のリンク回路

１０１～１０４　パケット処理回路

２００～２０３　上位層インターフェース回路

３００，３０２　暗号処理回路

４００　記録再生装置

５００　ＣＰＵ

５０１　ＲＯＭ

５０２　ＲＡＭ

７００　　１３９４ＰＨＹチップ

７１１～７１３　１３９４ＰＨＹポート

７２１～７２２　１３９４ソケット

７３１～７３３，７５１～７５３　１３９４プラグ

７４１，７４２　１３９４ケーブル

７２０　ＩＥＥＥ１３９４規格のコネクタ部

７３０　ＩＥＥＥ１３９４規格のケーブル

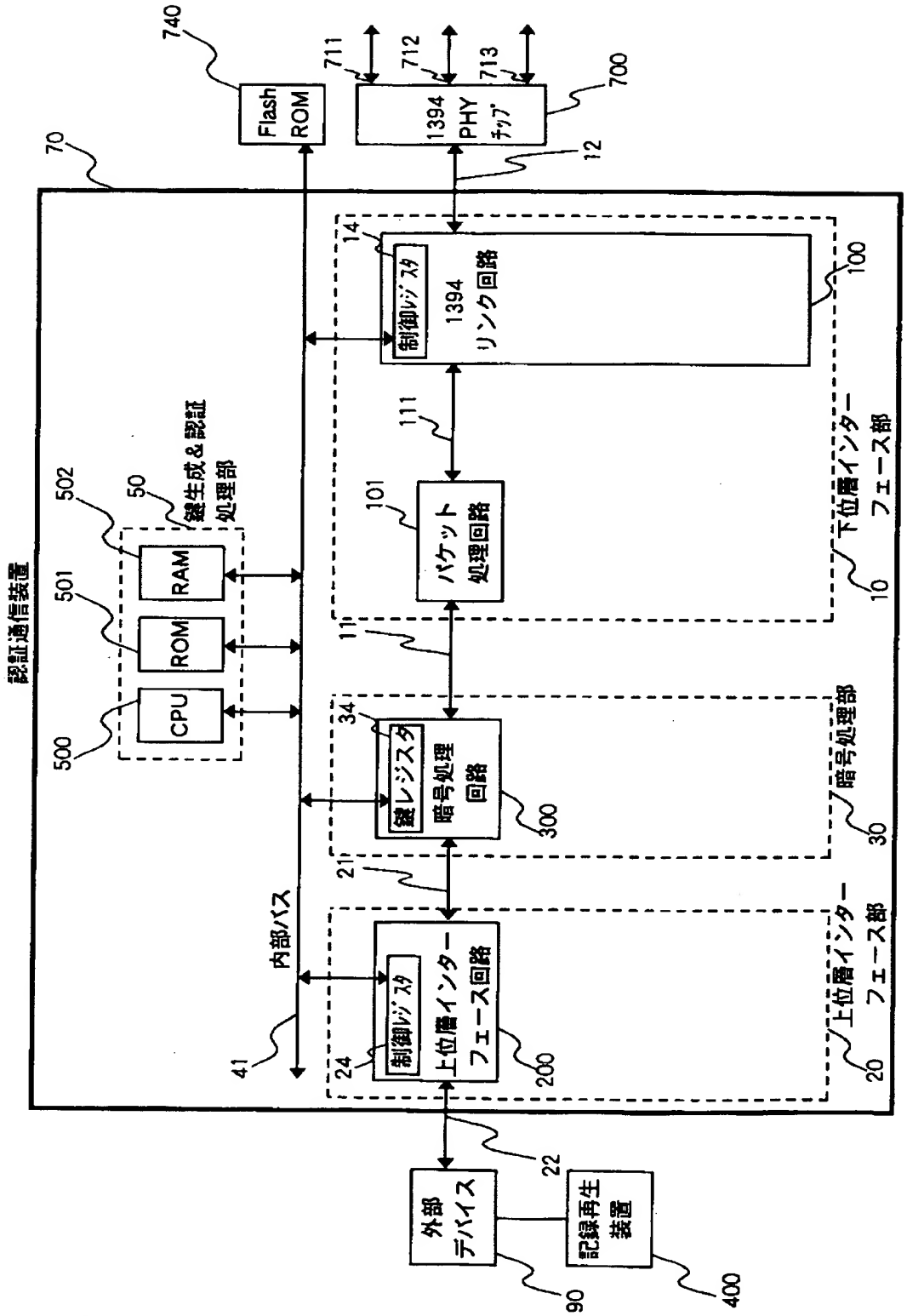
７４０　外部メモリ（フラッシュＲＯＭ）

８００，８００Ａ，８００Ｂ　ＡＶ機器

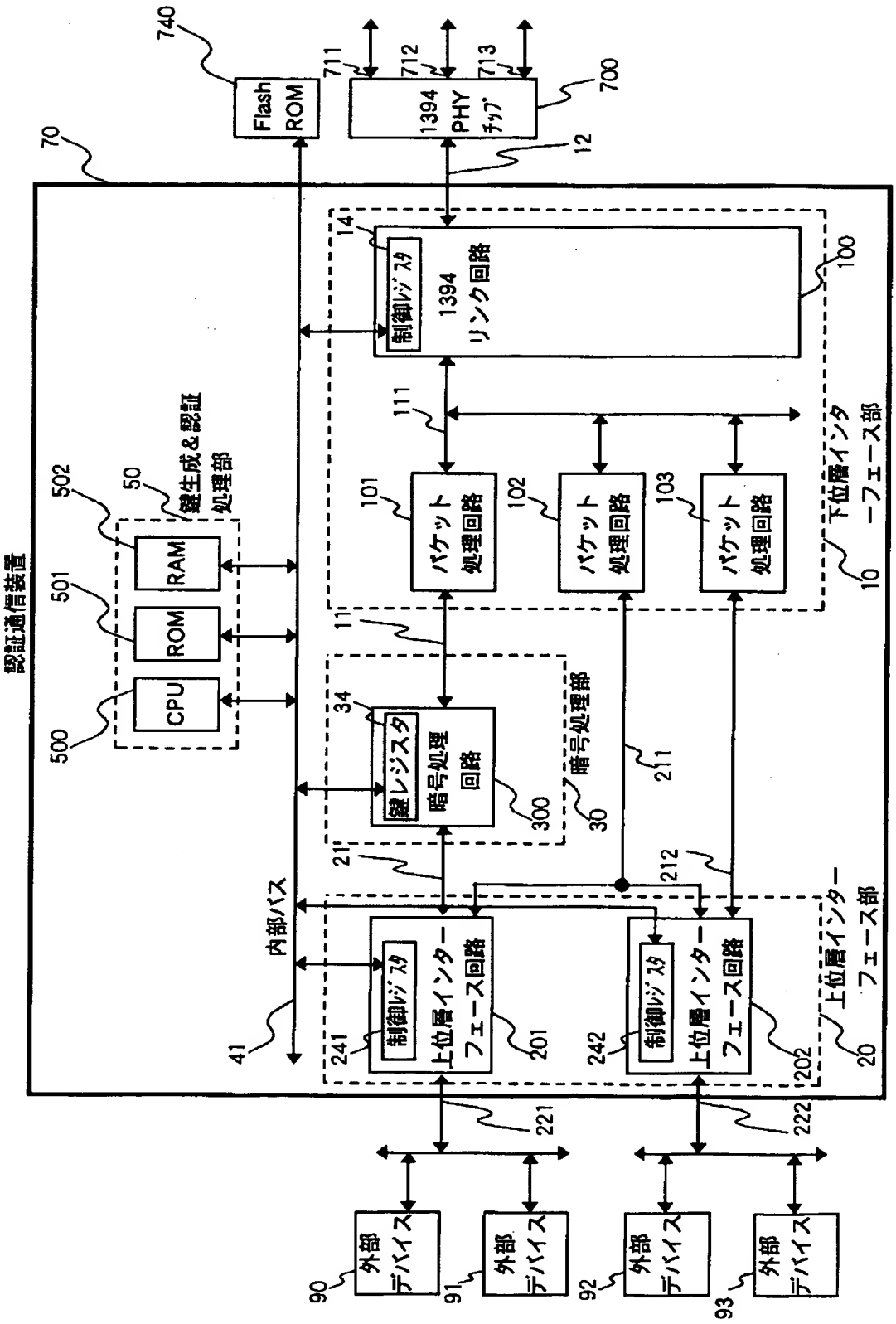
８１０　ＩＥＥＥ１３９４規格のバス

【書類名】　　図面

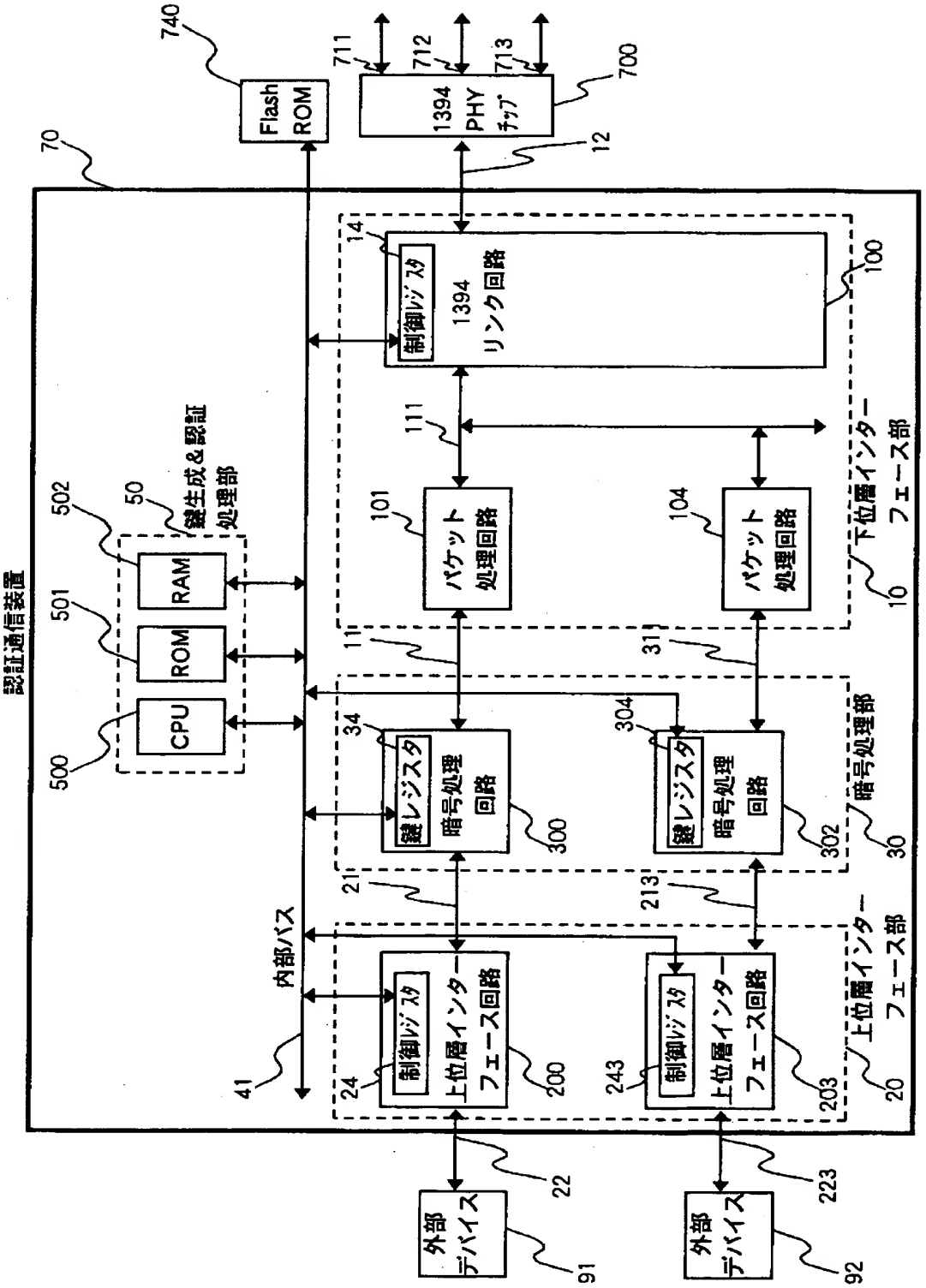
【図１】


740
Flash ROM
711
712
713
700
1394 PHY チップ
70
12
14
制御レジスタ
1394 リンク回路
100
下位層インターフェース部
10
111
101
パケット処理回路
11
認証通信装置
502
50
鍵生成＆認証処理部
RAM
501
ROM
CPU
500
34
鍵レジスタ
暗号処理回路
300
暗号処理部
30
21
内部バス
制御レジスタ
上位層インターフェース回路
200
24
41
上位層インターフェース部
20
22
外部デバイス
90
記録再生装置
400

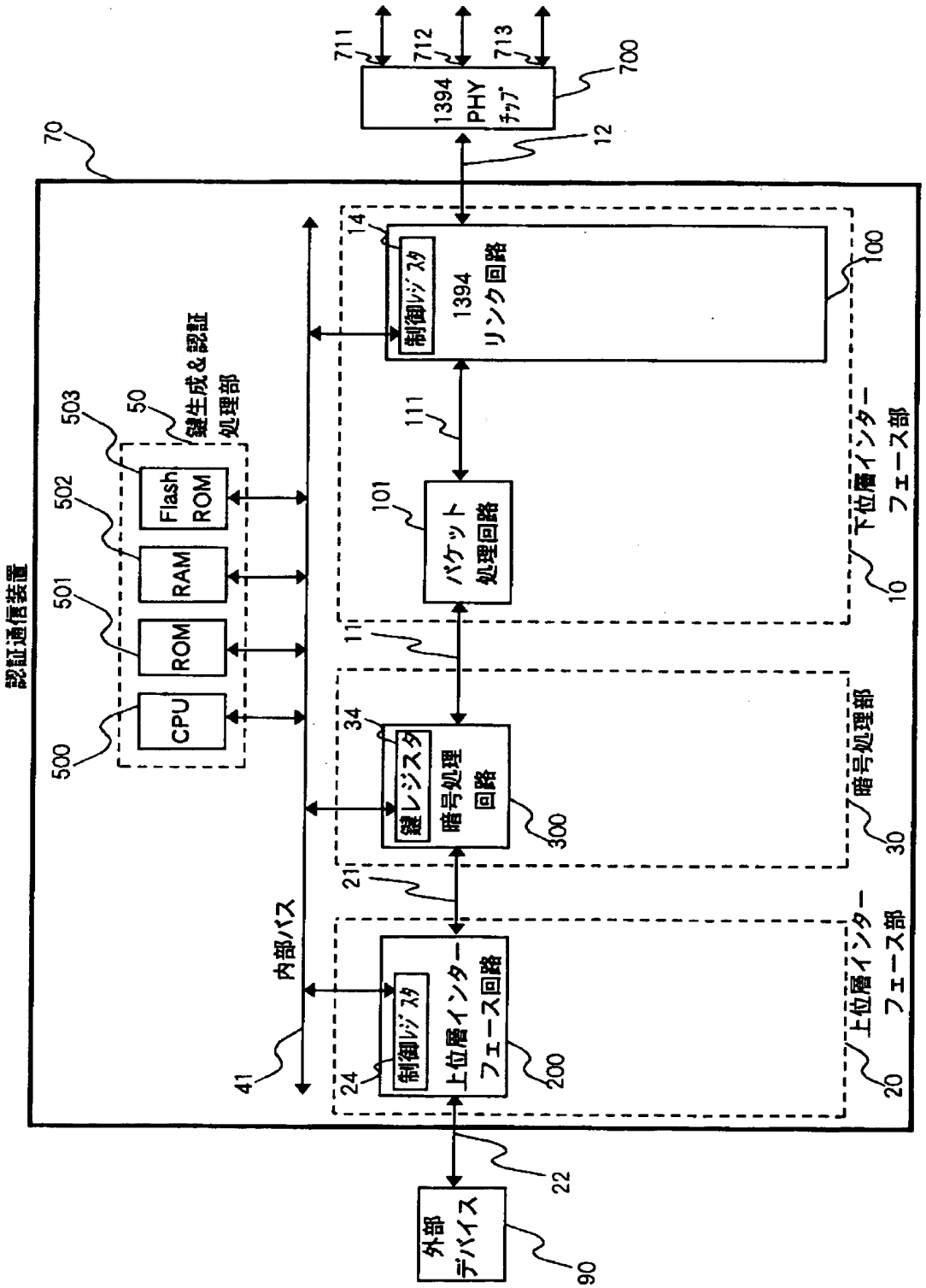
【図２】


認証通信装置
70
740
Flash ROM
711
712
713
700
1394 PHY チップ
12
14
制御レジスタ
1394 リンク回路
100
111
101
102
103
パケット処理回路
パケット処理回路
パケット処理回路
下位層インターフェース部
10
11
50
鍵生成＆認証処理部
502
501
500
RAM
ROM
CPU
34
鍵レジスタ
暗号処理回路
300
暗号処理部
30
211
21
212
内部バス
41
241
制御レジスタ
上位層インターフェース回路
201
242
制御レジスタ
上位層インターフェース回路
202
上位層インターフェース部
20
221
222
外部デバイス
外部デバイス
外部デバイス
外部デバイス
90
91
92
93

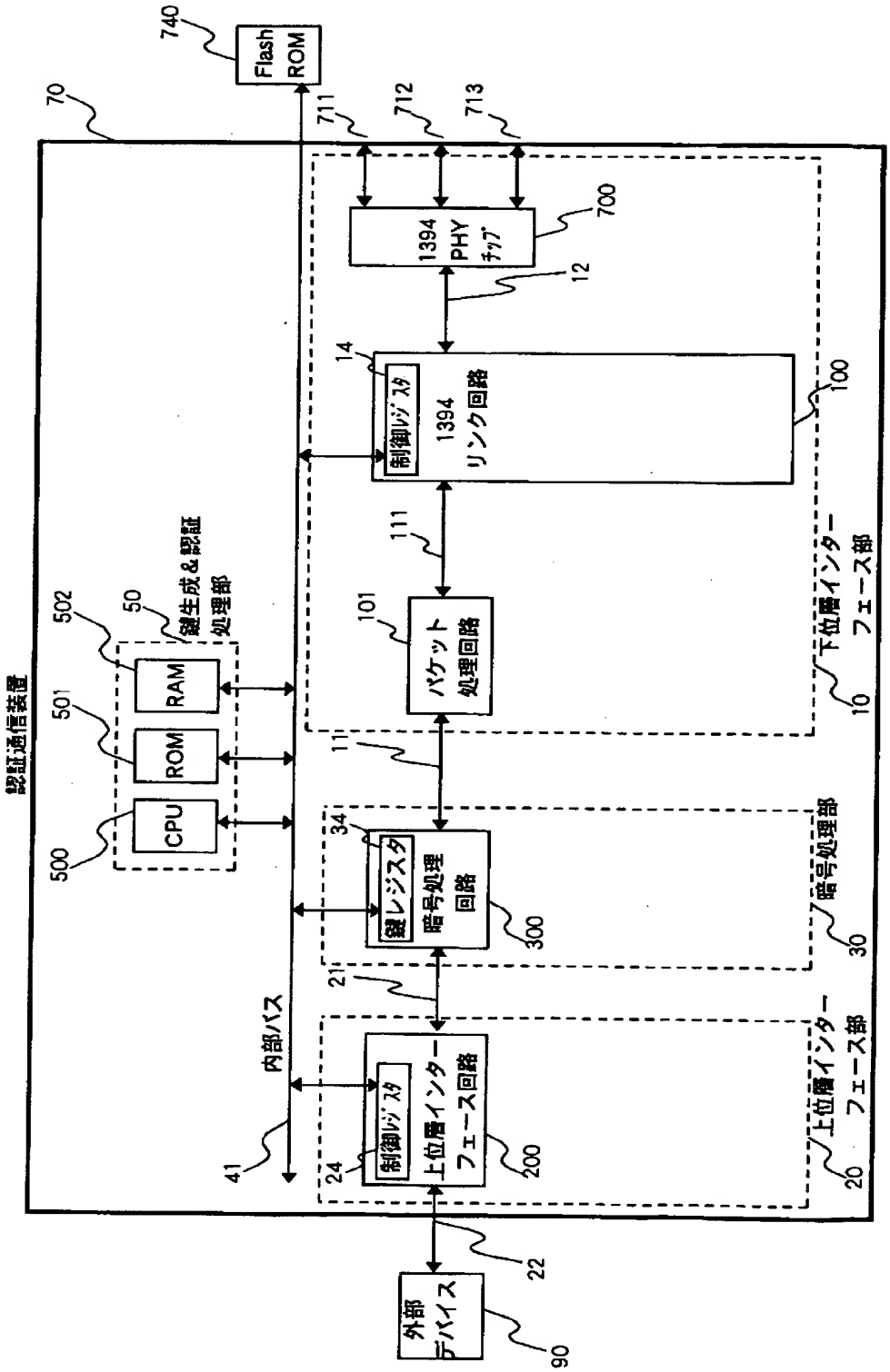
【図３】


認証通信装置
70
Flash ROM
740
1394 PHY チップ
700
711
712
713
12
100
1394 リンク回路
制御レジスタ
14
111
下位層インターフェース部
10
パケット処理回路
101
パケット処理回路
104
鍵生成＆認証処理部
50
RAM
502
ROM
501
CPU
500
11
31
暗号処理部
30
鍵レジスタ
暗号処理回路
34
300
鍵レジスタ
暗号処理回路
304
302
21
213
内部バス
上位層インターフェース部
20
制御レジスタ
上位層インターフェース回路
24
200
制御レジスタ
上位層インターフェース回路
243
203
41
22
223
外部デバイス
91
外部デバイス
92

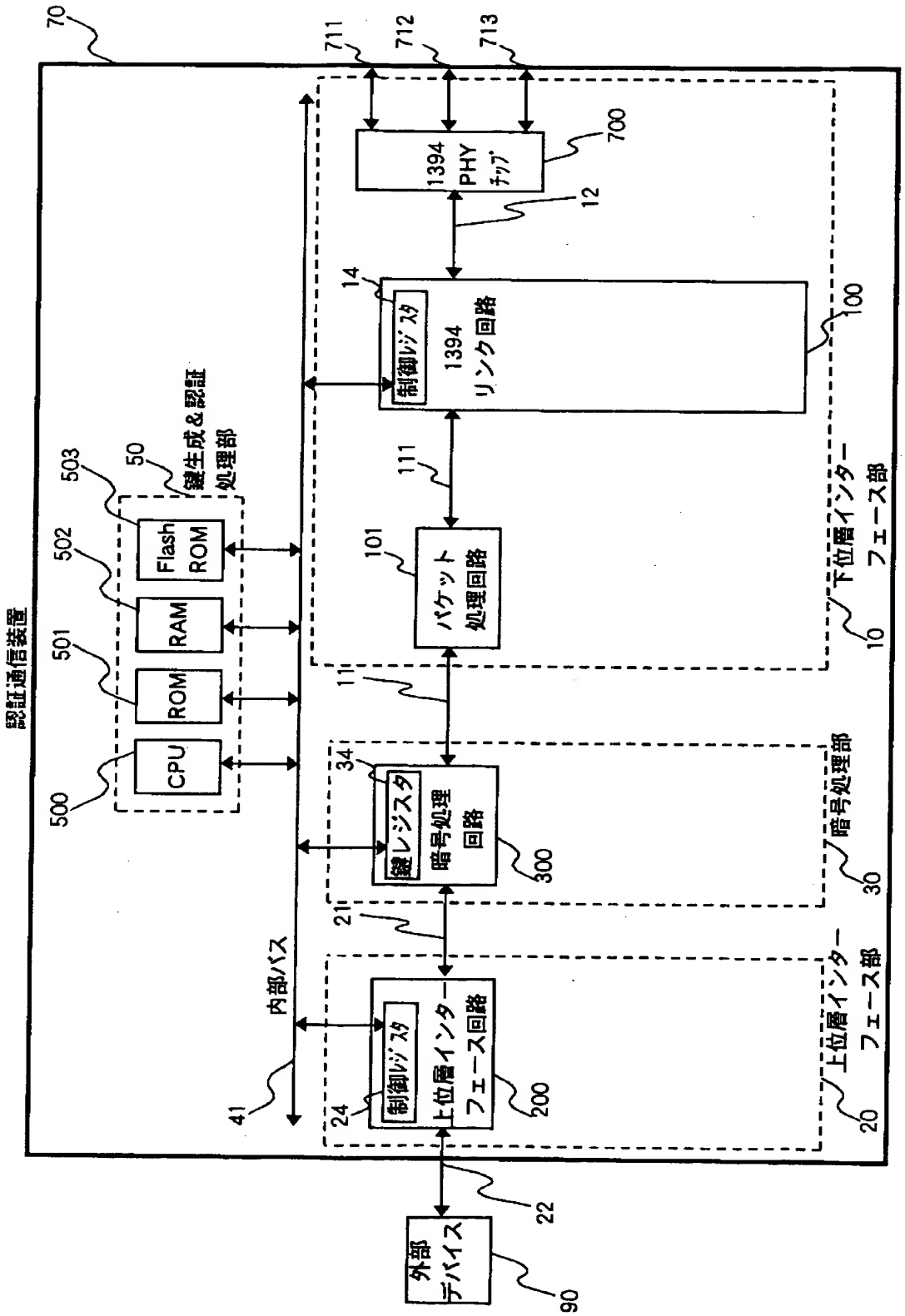
【図４】


認証通信装置
70
711
712
713
700
1394 PHY チップ
12
14
制御レジスタ
1394 リンク回路
100
下位層インターフェース部
10
111
101
パケット処理回路
11
鍵生成＆認証処理部
50
503
502
501
500
Flash ROM
RAM
ROM
CPU
34
鍵レジスタ
暗号処理回路
300
暗号処理部
30
21
内部バス
41
24
制御レジスタ
上位層インターフェース回路
200
上位層インターフェース部
20
22
外部デバイス
90

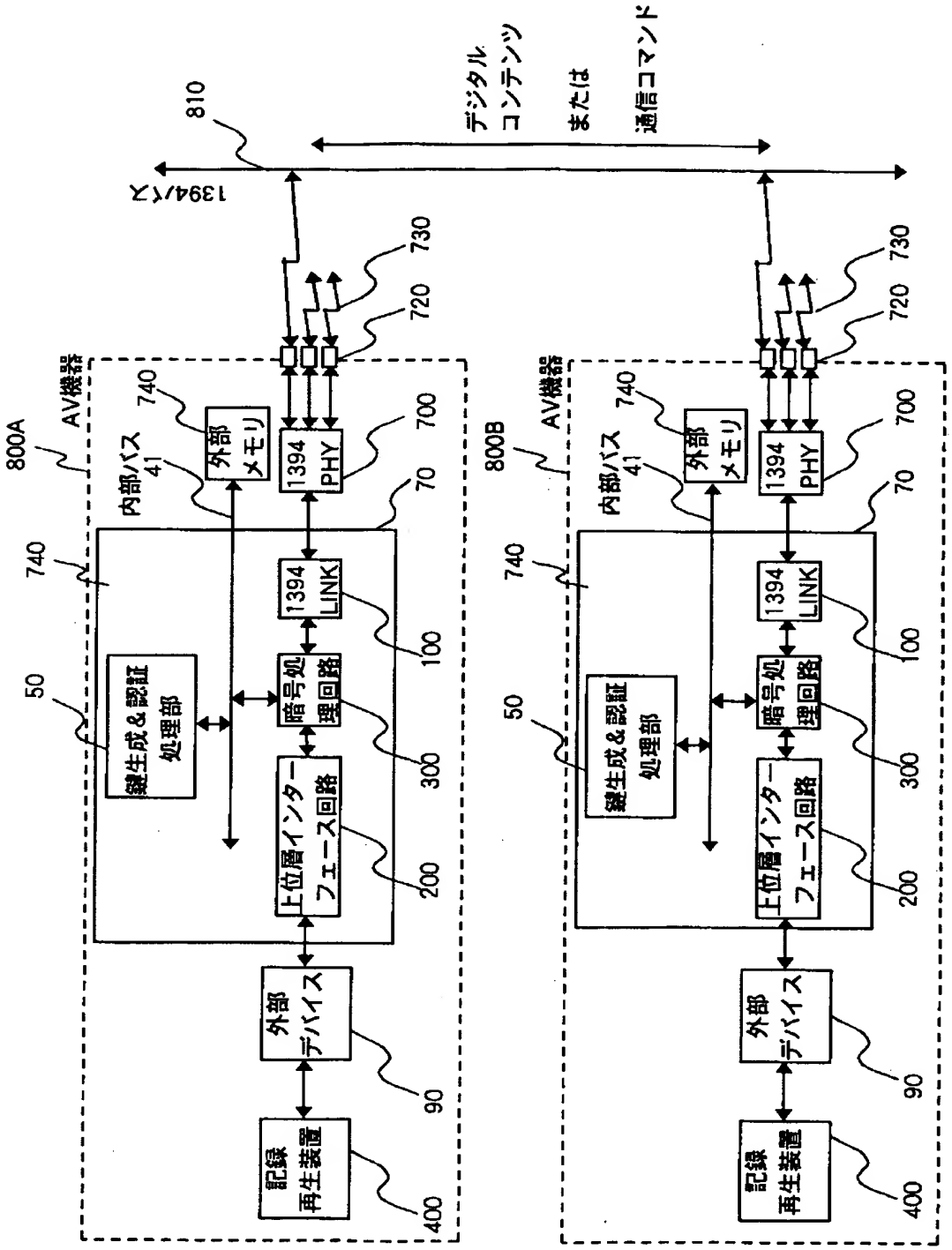
【図５】


認証通信装置
70
740
Flash ROM
711
712
713
1394 PHY チップ
700
12
14
制御レジスタ
1394 リンク回路
100
111
101
パケット 処理回路
下位層インター フェース部
10
11
50
鍵生成＆認証 処理部
502
501
500
RAM
ROM
CPU
34
鍵レジスタ
暗号処理 回路
300
暗号処理部
30
21
内部バス
41
24
制御レジスタ
上位層インター フェース回路
200
上位層インター フェース部
20
22
外部 デバイス
90

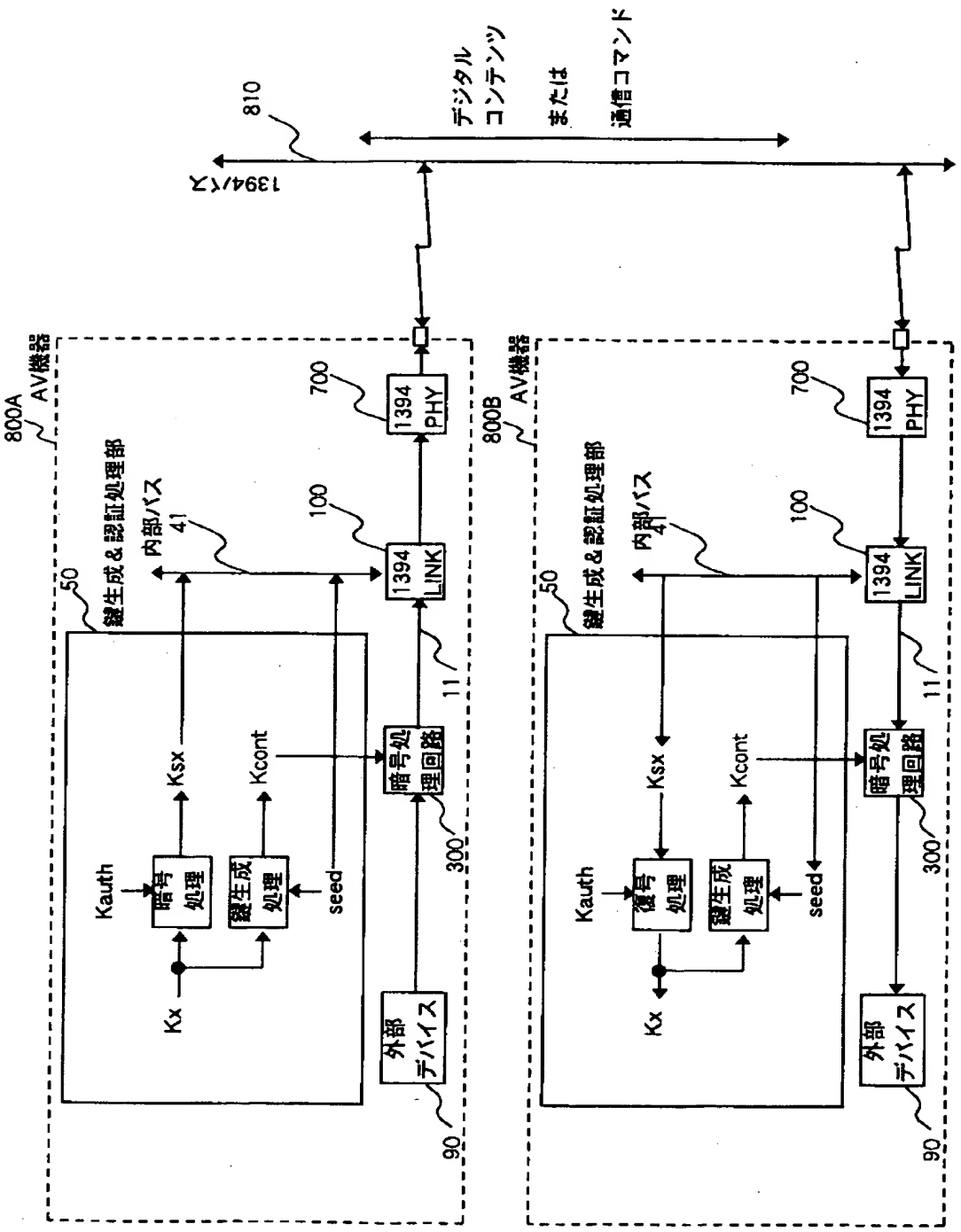
【図６】


70
711
712
713
700
1394 PHY チップ
12
14
制御レジスタ
1394 リンク回路
100
111
101
パケット処理回路
下位層インターフェース部
10
11
34
鍵レジスタ
暗号処理回路
300
暗号処理部
30
21
内部バス
制御レジスタ
上位層インターフェース回路
200
上位層インターフェース部
20
41
24
22
外部デバイス
90
認証通信装置
鍵生成＆認証処理部
50
503
Flash ROM
502
RAM
501
ROM
CPU
500

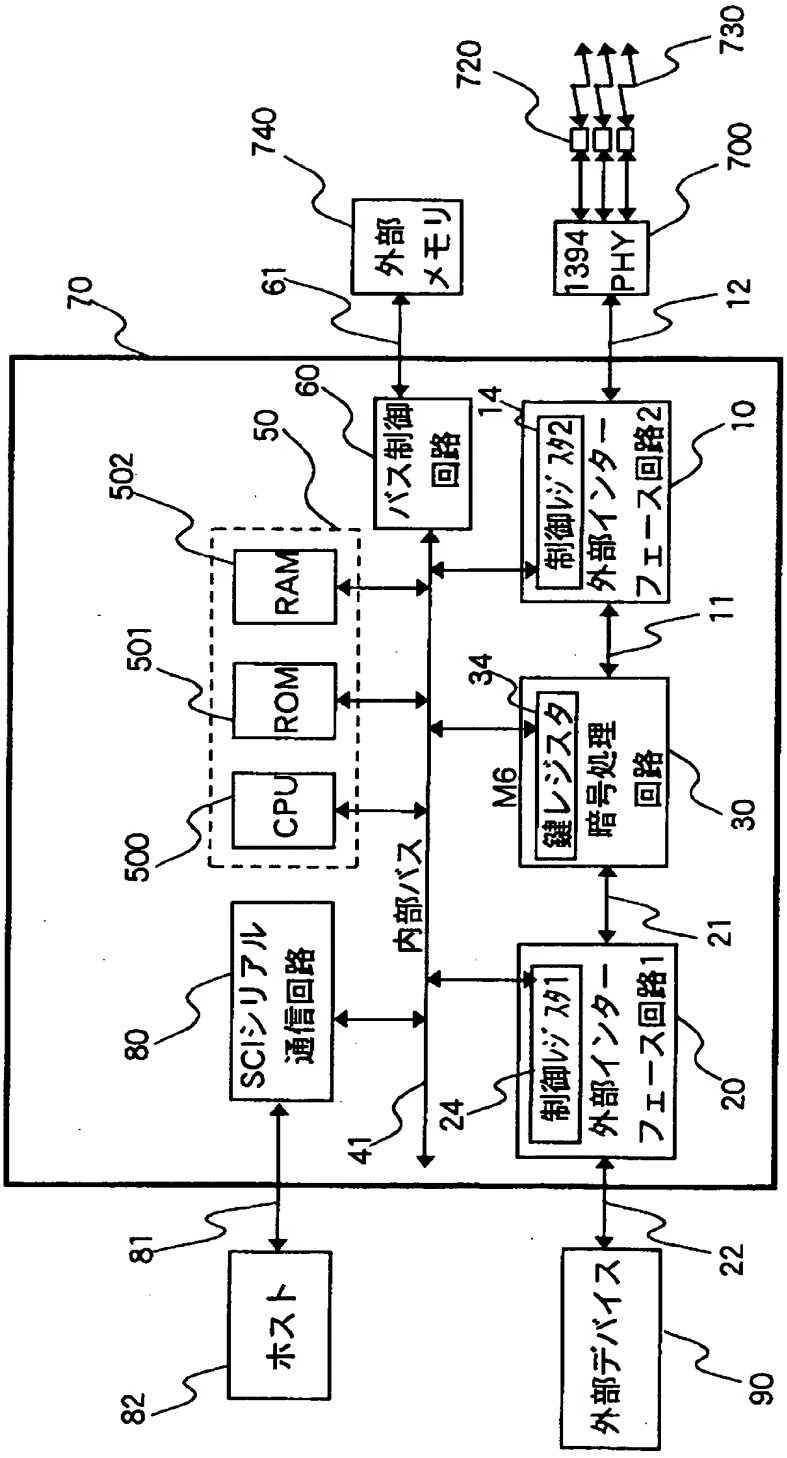
【図７】


デジタル
コンテンツ
または
通信コマンド
810
1394バス
730
720
AV機器
800A
740
外部
メモリ
1394
PHY
700
内部バス
41
70
1394
LINK
100
鍵生成＆認証
処理部
50
暗号処
理回路
300
上位層インター
フェース回路
200
外部
デバイス
90
記録
再生装置
400
AV機器
800B

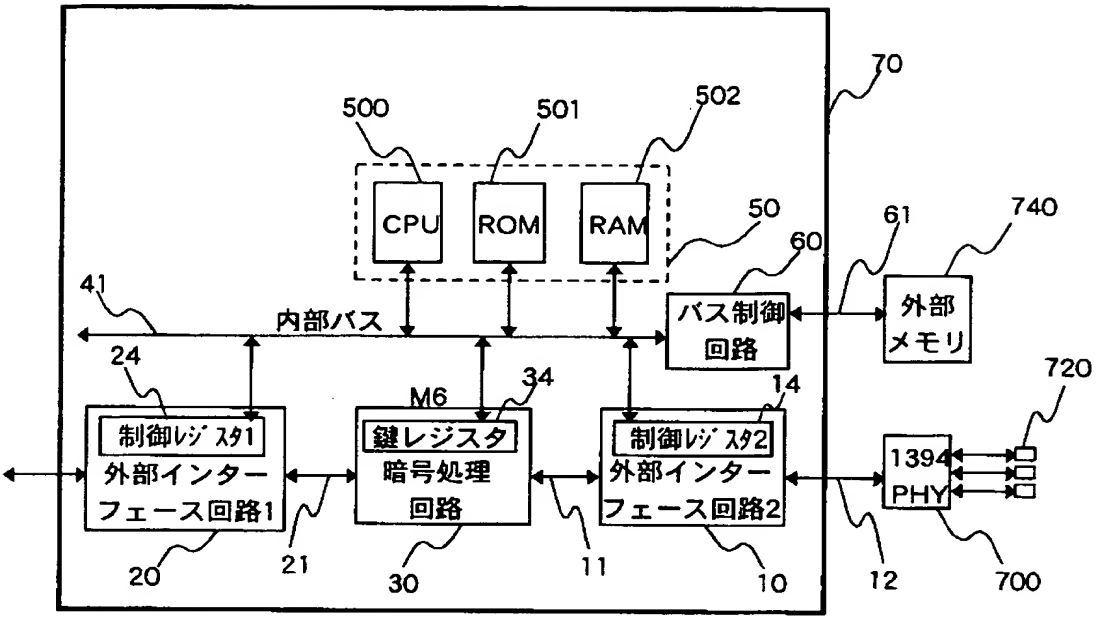
【図８】


810
デジタル
コンテンツ
または
通信コマンド
1394バス
800A
AV機器
800B
AV機器
700
1394
PHY
100
1394
LINK
11
内部バス
41
50
鍵生成＆認証処理部
Ksx
Kcont
Kauth
暗号
処理
鍵生成
処理
seed
Kx
暗号処
理回路
300
外部
デバイス
90
復号
処理

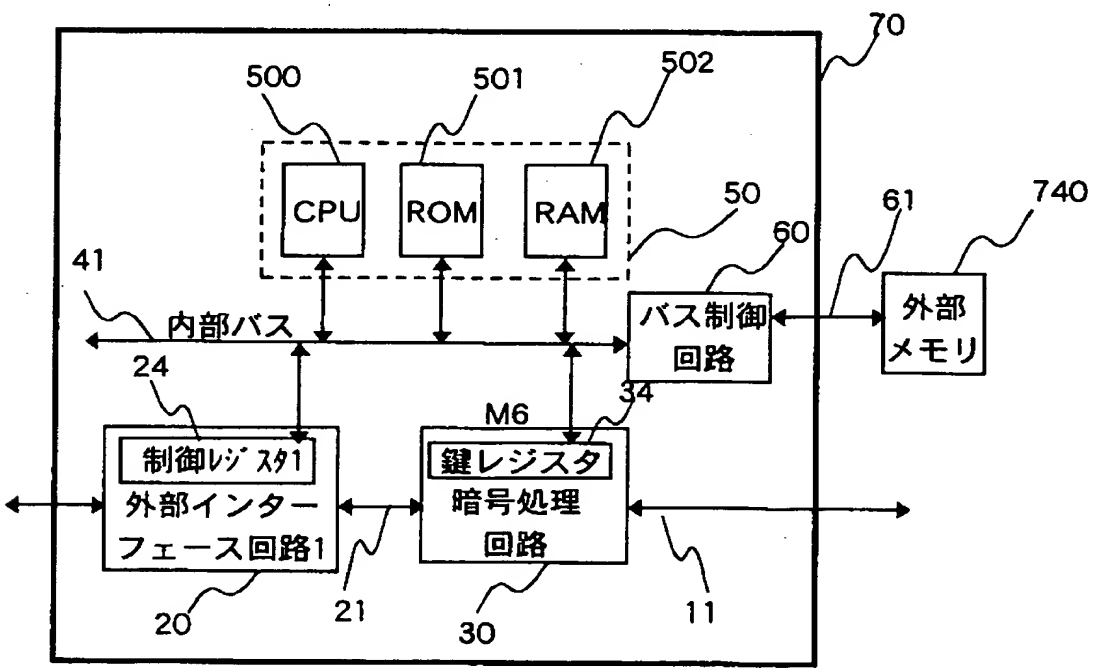
【図９】


720
730
740
700
外部メモリ
1394 PHY
61
12
70
60
バス制御回路
14
制御レジスタ2
外部インターフェース回路2
10
50
502
RAM
501
ROM
34
11
M6
鍵レジスタ
暗号処理回路
30
500
CPU
内部バス
21
80
SCIシリアル通信回路
制御レジスタ1
外部インターフェース回路1
20
24
41
81
22
ホスト
外部デバイス
82
90

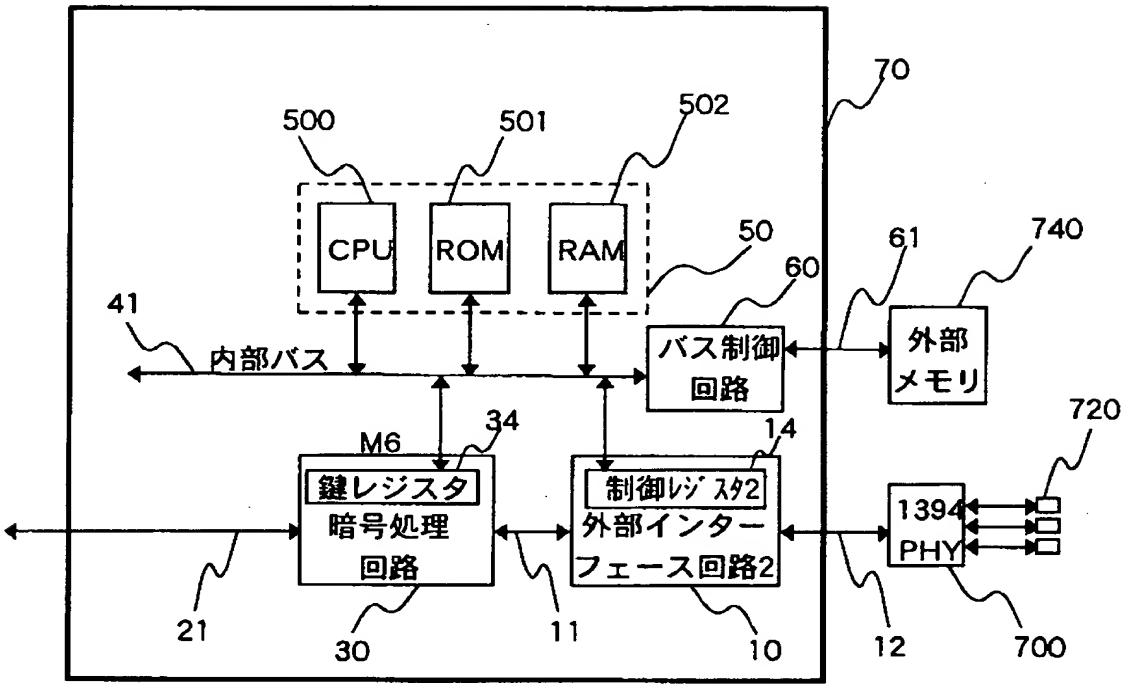
【図１０】


70
500
501
502
CPU
ROM
RAM
50
61
740
60
41
内部バス
バス制御
回路
外部
メモリ
24
M6
34
14
720
制御ﾚｼﾞｽﾀ1
鍵レジスタ
制御ﾚｼﾞｽﾀ2
1394
外部インター
フェース回路1
暗号処理
回路
外部インター
フェース回路2
PHY
20
21
30
11
10
12
700

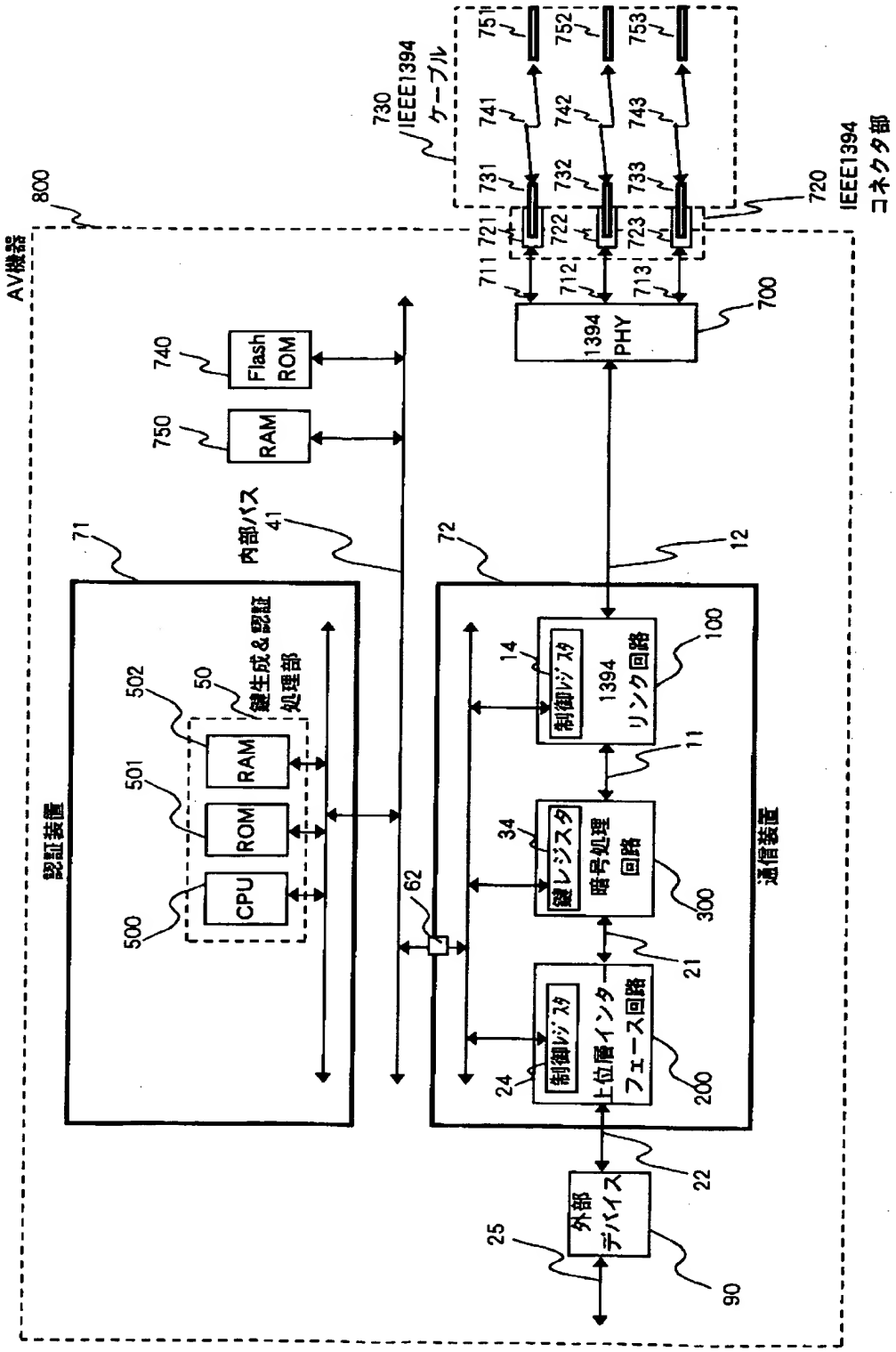
【図１１】


70
500
501
502
CPU
ROM
RAM
50
61
740
60
41
内部バス
バス制御
回路
外部
メモリ
24
M6
34
制御ﾚｼﾞｽﾀ1
鍵レジスタ
外部インター
フェース回路1
暗号処理
回路
20
21
30
11

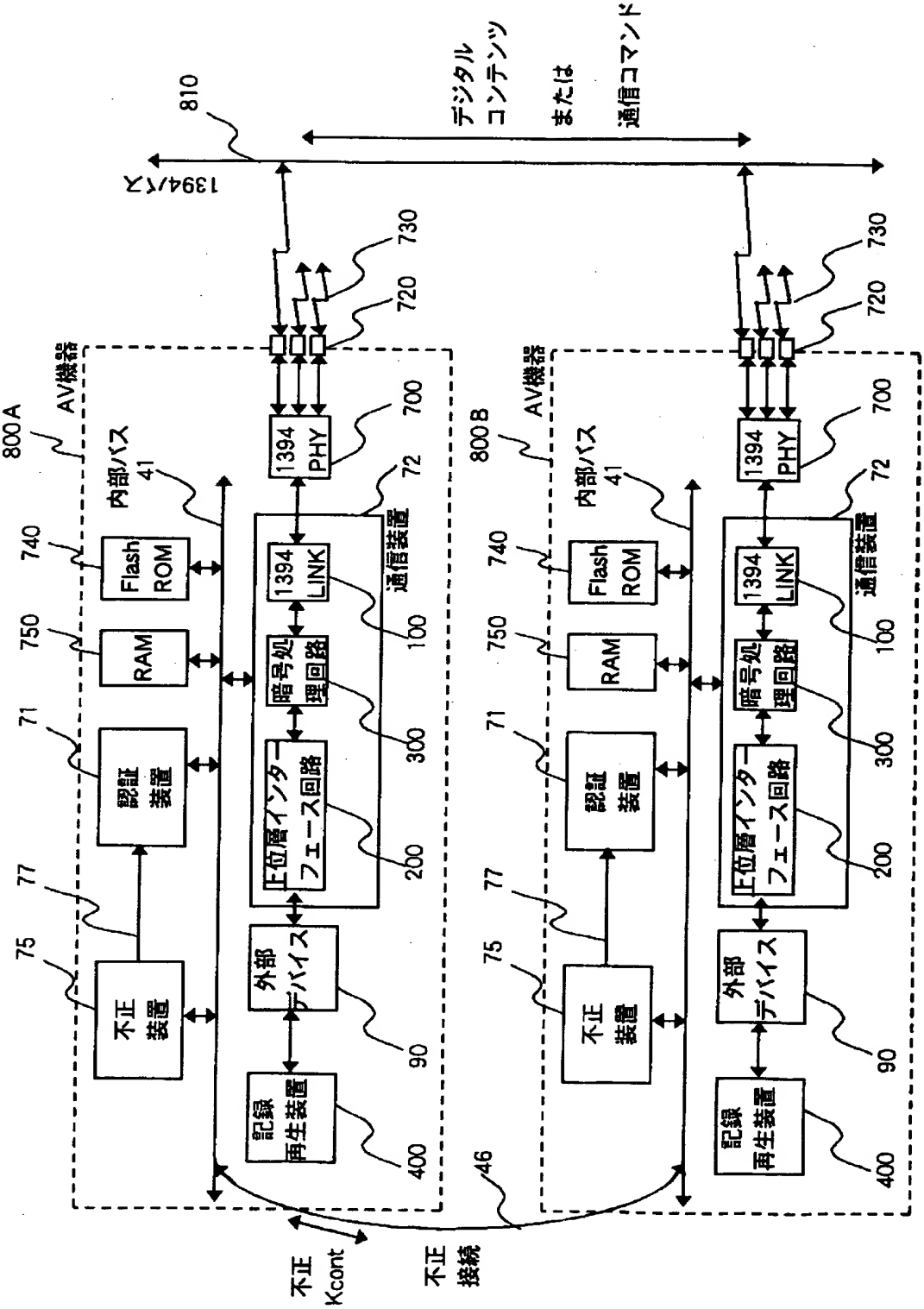
【図１２】


70
500
501
502
CPU
ROM
RAM
50
60
61
740
41
内部バス
バス制御
回路
外部
メモリ
720
M6
34
14
鍵レジスタ
暗号処理
回路
制御レジスタ2
外部インター
フェース回路2
1394
PHY
21
30
11
10
12
700

【図１３】


AV機器
800
IEEE1394
ケーブル
730
IEEE1394
コネクタ部
720
751
752
753
741
742
743
731
732
733
721
722
723
711
712
713
1394
PHY
700
Flash
ROM
740
RAM
750
内部バス
41
71
72
12
認証装置
通信装置
鍵生成＆認証
処理部
50
502
501
500
RAM
ROM
CPU
62
14
制御レジスタ
1394
リンク回路
100
11
34
鍵レジスタ
暗号処理
回路
300
21
制御レジスタ
上位層インター
フェース回路
200
24
22
25
外部
デバイス
90

【図１４】


デジタル
コンテンツ
または
通信コマンド
810
1394バス
730
720
AV機器
800A
800B
内部バス
41
1394
PHY
700
72
通信装置
1394
LINK
100
暗号処理回路
300
上位層インターフェース回路
200
Flash
ROM
740
RAM
750
認証装置
71
不正装置
75
77
外部デバイス
90
記録再生装置
400
46
不正
Kcont
不正
接続

【書類名】　要約書

【要約】

【課題】　不正コピー防止の技術を破るため、ＣＰＵバスにロジック・アナライザのプローブを接続するなどして、認証処理過程を窃取し解析することで不正コピー防止の仕掛けを破られる可能性があった。また、ＣＰＵバスへ改竄された暗号鍵などを設定できるような電子機器の改造のおそれがあった。

【解決手段】　１個の半導体チップ上に、所定のアルゴリズムに従って鍵コードを生成するとともに外部装置とのデータの送受信の認可／非認可の決定並びに通信制御を行なう主処理部と、該処理部で生成された鍵コードを用いて送受信データの暗号化および復合化を行なう暗号処理部と、所定のプロトコルに従って上位層または下位層との通信を行なうインタフェース部とを形成して、暗号処理過程や認証処理過程での暗号鍵を装置の外部から窃取できにくくした。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２０００－１５８７７０
受付番号	５００００６６２０９６
書類名	特許願
担当官	第一担当上席　００９０
作成日	平成１２年　６月１４日

＜認定情報・付加情報＞

【提出日】　平成12年 5月29日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所